PERFORMANCE WORK STATEMENT (PWS)

for

Air Force Medical Operations Agency (AFMOA/SGDS)

DENTAL IMAGING COLLABORATIVE ENVIRONMENT (DICE) SUPPORT

ID05180037/Contract Number (TBD)

19 Sept 2018

PERFORMANCE WORK STATEMENT
DENTAL IMAGING COLLABORATIVE ENVIRONMENT (DICE) SUPPORT

1. DESRIPTION OF SERVICES

1.1. Government Mission and Objective. The Air Force Medical Operations Agency, Dental Directorate (AFMOA/SGD) is the office of responsibility for United States Air Force (USAF) dental operations and sustainment. AFMOA/SGD provides a full spectrum of dental services to 520,000 eligible military and retired beneficiaries in the Continental United States (CONUS) and Outside Continental United States (OCONUS) permanent locations and to the joint war fighters at deployed locations around the world. The purpose of this requirement is to strategically integrate and sustain cost-effective dental technology solutions that enhance the Military Healthcare System (MHS) by employing Commercial-Off-the-Shelf (COTS) software with dental equipment that improves access to high quality care and aids in cost reduction. The Air Force Dental Information and Technology Action Group (AF DITAG) provides total lifecycle management of all dental technologies enabling "Trusted Care, Anywhere," the Air Force Medical Service (AFMS) prime target. The AFMS strategy identifies four (4) strategic goals of "Readiness, Better Care, and Better Health at the Best Value." This requirement enables the Air Force Dental Service (AFDS) to deliver state-of-the-art technology to its dental surgeons so they may ensure readiness while providing better care that leads to better health.

1.1.1. Project History and Expansion. The AF DITAG began as a single-solution provider for two-dimensional (2D) radiography. Beginning in 2006, using a COTS program known as Medicor Imaging Picture Archive Communication System (MiPACS), the previous AF Digital Dental Radiology Solution/Dental Imaging Collaborative Environment (DDRS) team deployed a globally available digital dental radiography solution that is fully compatible with medical radiology standards (Digital Imaging and Communications in Medicine/ Picture Archive and Communication System (DICOM/PACS)). The current effort recognizes the scope of dental technology has expanded to include many new, essential capabilities: three-dimensional (3D) radiography, visible light photography, software/hardware specific to the dental specialties, and electronic solutions for dental radiology reading service and dental laboratory ordering and workflow. Each of these technologies plus future solutions must be integrated together so that the Dental Electronic Health Record (D-EHR) (Dentrix Enterprise) functions as the "System of Record" for the patient.

1.2. Scope of Work. This requirement is for non-personal, Dental IT services in support of AFMOA/SGD to servicing 176 Military Treatment Facilities (MTFs) to include AF, Air Force Reserve Command (AFRC) and Air National Guard (ANG). The Contractor shall establish a Contractor team to assist in the management of all current and pre-defined future technologies to include all aspects of architecture, integration and sustainment of the whole suite of AF Dental Information and Technology (DIT) ensuring maximized efficiencies and provide the AF Dental Information and Technology Program Office (AF DITPMO) with a Contractor team to implement and assist with management of high availability tools that are critical to patient care. The Contractor shall perform a full range of technical and administrative services as required. Government personnel will be available to provide technical input, answer questions, review completed draft deliverables, provide feedback, and provide shipping directions for deliverables. Some of the technologies managed by AF DITAG are used by ANG Dental Flights, therefore one (1) or more Contractor team members are funded by the ANG to provide a high level of support to

their units while being embedded in the broader team.

2. GENERAL INFORMATION

2.1. Contractor Identification. All Contractor/Subcontractor personnel shall identify themselves as Government Contractor personnel during all forms of communications such as business meetings, telephone conversations, electronic mail, attendance sheets, coordination documentations, reports, and the signature blocks utilized in all correspondence. If a contract requires Government workspace, the Contractor personnel shall wear a picture identification badge and identify their workspace area with their name and company affiliation.

2.2. Contractor Training:

2.2.1. Government-Furnished Training. Contract employees shall attend all such Government provided training as part of normal services required and billed under the contract. The contractor employee may be required to complete additional training in addition to the web-based training listed below:

2.2.1.1. Department of Defense (DoD) Information Assurance Cyber Awareness Challenge (ADLS Course)

2.2.1.2. Environmental Management Systems (EMS) – General Awareness Training

2.2.1.3. Security Administration (ADLS Course)

2.2.1.4. Health Insurance Portability and Accountability Act (HIPAA) and Privacy Act Training (JKO Course)

2.2.1.5. Operation OPSEC Awareness Training (ADLS Course)

2.2.1.6. Derivative Classification and Marking Classified Information

2.3. Contractor/Government Communication. The Contractor shall designate a Focal Point to be the single point of contact (POC) for all Contractor and Government correspondence. The Focal Point shall provide clear and consistent written and verbal response to Government within 24 hours of Government initiated communication (e.g., return phone calls, emails or other communication). The Contractor's Focal Point shall meet with the Government team at least monthly, and additional meetings may be requested by the Government or the Contractor as necessary. The Contractor Focal Point, Contract Officers' Representative (CORs) and/or other designated representative will provide monthly performance feedback to the Contractor. The Contractor shall provide a meeting agenda and minutes.

2.4. Personnel Retention and Recruitment. The Contractor shall make every effort to retain personnel in order to ensure continuity until contract completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. The Contractor shall submit the resume(s) of all potential personnel selected to perform under this contract to the COR through email, or any other process means identified/required, for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. This may necessitate the use of temporary employees to fill short term gaps between permanently assigned employees. Long-term absences are considered those

longer than two weeks in duration.

2.5. Place of Performance: The primary place of performance shall be in Contractor facilities or via telework. However, one FTE shall be located within 50 miles of Wright Patterson AFB. Additional FTEs may be required to be located within 50 miles at any of the AF and Defense Health Agency (DHA) Government locations listed below. As required, the Contractor shall perform work at the Government locations listed below or may be advised by the COR or Project Manager of other required locations as designated by AFMOA/SGD. Temporary duty locations may include any DoD, Air Force, Air National Guard or Air Force Reserve Command installation having AF DIT equipment within the CONUS or OCONUS. Primary Government locations are listed below. Travel to locations will be authorized to all locations with the exception of the one FTE located at Wright Patterson AFB.

AFMOA/SGD
3515 S. General McMullen Dr.
Building 1, Bay 2, Suite 1023
San Antonio, Texas 78226

Wright Patterson Medical Center
4881 Sugar Maple Drive B830
Wright Patterson AFB, OH 45433

MESOC-SATX DHA Data Center
Bank of America Plaza, STE 300
San Antonio TX 78205

MESOC-AUCO DHA Data Center
16401 East Centretech Parkway,
Aurora, CO 80011

2.6. Period of Performance. The period of performance for this task order will be a one year base and four one year options. The anticipated period of performance is below.

Base Year (includes Phase In): February 28, 2019 to February 27, 2020
Option Year 1: February 28, 2020 to February 27, 2021
Option Year 2: February 28, 2021 to February 27, 2022
Option Year 3: February 28, 2022 to February 27, 2023
Option Year 4: February 28, 2023 to February 27, 2024

2.7. Phase-In Plan. The Phase-In period shall be a 30 day period after the period of performance starts. The contractor shall provide a Phase-In Plan that shall include the following information/details, at a minimum:

2.7.1. The initial 15 days of the 30 day period will allow for new personnel to be on-site, shadowing the full incumbent staff. The full incumbent staff is accountable for full performance of the PWS. Activities shall include reviewing day-to-day operations, procedures and protocols, Operations Lead/PM (incumbent and new contractor) attending weekly transition meetings with

Government PM/COR, and Government Technical Lead with status, questions and concerns with the Government and outgoing contractor.

2.7.2. The last 15 days of the 30 day period will allow for a reverse transition. All new contractor staff shall be on-site and accountable for full performance of the PWS. The incumbent contractor will stay on-site in a strictly consulting capacity for the new contractor.

2.7.3. Phase-Out period.

2.7.4. The phase out period consists of 30 days prior to the expiration of the task order. The contractor shall perform the following activities for the phase-out period:

2.7.5. Ensure all services and performance objectives required by the PWS and Task Order PWS's are met throughout the phase-out periodEstablish procedures with the successor to ensure transition of provided services without a degradation of service

2.7.6. Provide the successor with copies of all instructions, records, databases, contract performance metric data, vendor points of contact, and all other procedures developed by the contractor in the performance of this contract

2.8. Duty Hours:

2.8.1. Normal operational hours are 0700 to 1700 (CST) (staggering shifts), Monday through Friday, excluding government-observed holidays. Contractors shall be available during the core hours of 0900 to 1500 (CST).

2.8.2. Normal workdays are Monday through Friday for the AF team except for US Federal Holidays. Normal workdays for the ANG Support position are Thursday – Monday for drill weekends and Monday – Friday for non-drill weekends, with adjustment for US Federal Holidays, but may be adjusted to meet mission requirements. This schedule optimizes the time that the ANG Support personnel is able to work with the ANG Systems Flights that work a Monday – Friday schedule.

2.8.3. Contractor personnel normally work eight (8) hours per day. However, short-term surge situations may make performance in excess of eight (8) hours per day necessary on occasion. If this occurs, the Contractor can work flex time. This may include weekend work, the Contractor shall ensure they can provide for this type of contingency. Normal work hours for the AF are based on flextime. For ANG sites normal/core work hours during drill weekends are from 0900 to 1800 EST to ensure coverage across US time zones. Contractor employees supporting the ANG work are expected to be available during ANG core hours.

2.8.4. In the event the Government has a requirement for expedited performance or extended work days to meet schedule constraints or work volume, the Government shall communicate those needs to the Contractor and they shall ensure adequate labor resources to meet the schedule constraints. Should task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours, if so required.

2.8.5. The Contractor may perform work outside the normal duty hours at its own business location(s) or at the Government furnished facilities, when so authorized by the Government. The Contractor personnel working at Government facilities shall observe federal holidays and base closures on the same dates and during the same times as the Government personnel, since Contractor employees shall not have access to the Government facilities during these days and/or times

2.9. Federal Holidays: Federal offices are closed on New Year's Day, Dr. Martin Luther King Jr. Day, Presidents Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day. In addition, the Contractor will not have access to Government facilities on Family/Down Days. The COR will notify the Contractor of non-planned closures.

2.10. Telework/Telecommuting. Telework/telecommuting is the primary method of accomplishing the work effort under this PWS with occasional site-based work on an as required basis. However, one FTE will be required to be within 50 miles of Wright Patterson AFB. Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the award. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities. The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:
2.10.1. Controlling access to agency information and information systems;Protecting agency information (including personally identifiable information) and information systems;Limiting the introduction of vulnerabilities.
2.10.2. Protecting information systems not under the control of the agency that are used for teleworking.
2.10.3. Safeguarding wireless and other telecommunications capabilities that are used for teleworking.
2.10.4. Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

2.11. Base Closures:

2.11.1. In the event of an unplanned closure of a Government facility for any reason (e.g. natural disasters, military emergency, and Government shut-down, or severe weather) the Contractor shall make its best effort to mitigate loss of work time. If Contractor personnel are working on the Government installation, they should plan to telework from an off-site location to continue essential technical support services.

2.11.2. All Contractor personnel performing under this contract have been determined to be non-essential and are not to report to their AFB duty location during a base closure. Should the base be closed, the Contractor shall be notified by either the Contracting Officer, Air Force Technical Representative, or a local television or radio station. The Contractor is responsible for notifying its employees about base closures. Contractor employees are not to report to the base if it is closed and shall adhere to delays, unless otherwise specifically instructed otherwise by the CO or COR. This latter case would only be necessary if it is determined that Contractor operations are necessary to support crisis operations per DoD Instruction (DoDI) 3020.37, Continuation of Essential DoD Contractor Services during a Crisis, and Air Force implementation thereof.

2.11.3. Unplanned Facility Closures. The Contractor shall continue performance of services during unplanned closures of the facility due to natural disasters, military emergencies or severe weather. The Contractor shall not report to a Government facility when a base closure is in effect. The contractor shall coordinate their plan to continue services with the COR.

2.11.4. Travel Requirements.

2.11.5. Travel may be required during the performance period of this contract at the request of the Government and within the CONUS or OCONUS. Travel shall be required on occasion to conduct research observations; to attend meetings, symposiums, conferences, staff visits, either locally or nationally; or at other associated locations assigned to collect data, information and to validate studies and institutional memory for the AFMOA. The Government will require travel to perform services on site as required at the locations listed in 2.5 and any of the temporary remote duty locations for operational support, such as installing upgrades, troubleshooting, maintaining the system, and to provide training.

2.11.6. Projected travel is shown below for the base period of the contract and may be subject to change. The projected travel for each of the option periods is the same as shown below with the dates to be determined (TBD):

Projected Travel				
Event	**Projected Dates of Travel**	**Destination To/From**	**No. of Travelers**	**Duration**
(ISC)2 Gov't Security Summit	20 & 24 May 2019	Dayton OH / Washington DC (DCA)	1	5
(ISC)2 Gov't Security Summit	21 & 24 May 2019	Portland OR / Washington DC (DCA)	1	5
(ISC)2 Security Congress	Sep-19	Dayton OH /Las Vegas NV (LAS)	1	5
(ISC)2 Security Congress	Oct-19	Portland OR /Las Vegas NV (LAS)	1	5
VM World Conference	26 & 31 Aug 2019	Tampa FL/Las Vegas NV (LAS)	1	6

VM World Conference	27 & 31 Aug 2019	Portland OR/Las Vegas NV (LAS)	1	6
EMC World	30 Apr & 5 May 2019	Tampa FL Las Vegas NV (LAS)	1	6
EMC World	31 Apr & 5 May 2019	Portland OR Las Vegas NV (LAS)	1	6
Chicago Mid Winter Dental Mtg	21 & 25 Feb 2020	Dayton OH/Chicago IL (ORD)	1	5
Chicago Mid Winter Dental Mtg	22 & 25 Feb 2020	Portland OR/Chicago IL (ORD)	1	5
MiPACS User Mtg	June 2019	Dayton OH /Charlotte NC (CLT)	3	5
MiPACS User Mtg	June 2019	San Antonio TX / Charlotte, NC (CLT)	2	5
MiPACS User Mtg	June 2019	Portland, OR/ Charlotte, NC (CLT)	1	5
MiPACS User Mtg	June 2019	Tampa FL/ Charlotte, NC (CLT)	1	5
MiPACS User Mtg	June 2019	Ft Meyers FL/ Charlotte, NC (CLT)	1	5
MiPACS User Mtg	June 2019	Salt Lake City UT/ Charlotte, NC (CLT)	1	5
MiPACS User Mtg	June 2019	Austin TX/ Charlotte, NC (CLT)	1	5
ADA Annual Meeting	5 & 9 Sep 2019	Dayton OH/San Francisco CA (SFO)	1	5
ADA Annual Meeting	5 & 9 Sep 2019	Portland OR/San Francisco CA (SFO)	1	5
Ldrshp Mtg (SA)	TBD 2019	Dayton OH /San Antonio TX (SAT)	4	6
Ldrshp Mtg (SA)	TBD 2019	Portland, OR /San Antonio TX (SAT)	4	6
Ldrshp Mtg (SA)	TBD 2020	Tampa FL/San Antonio TX (SAT)	4	6
Ldrshp Mtg (DC)	TBD 2019	Portland OR/DC (DCA)	2	6
Ldrshp Mtg (DC)	TBD 2019	Dayton OH/DC (DCA)	2	6
Emergency Site Visit	TBD 2019	Portland OR/Keesler AFB MS (GPT)	1	3
Emergency Site Visit	TBD 2019	Tampa FL/Hanscom AFB MA (BOS)	1	3
Emergency Site Visit	TBD 2019	Salt Lake City UT/Lakenheath AFB (NWI)	2	5

Emergency Site Visit	TBD 2019	Salt Lake City, UT/Tyndall AFB (TCP)	1	5
Emergency Site Visit	TBD 2020	Salt Lake City, UT/Anderson AFB Guam (GUM)	1	5
Emergency Site Visit	TBD 2020	Salt Lake City UT/Misawa AB Japan (MSJ)	1	5
Project Travel	TBD 2019	Portland OR/Keesler AFB MS (GPT)	1	6
Project Travel	TBD 2019	Portland OR/Travis AFB CA 9 (SFO)	1	6
Project Travel	TBD 2019	Portland OR/Elemendorf AFB AK (ANC)	1	6
Project Travel	TBD 2019	Portland OR/Mountain Home AFB (BOI)	1	6
Project Travel	TBD 2019	Salt Lake City, UT/Kadena AB JP (OKA)	1	6
Project Travel	TBD 2019	Salt Lake City, UT/ McGuire AFB NJAFB (PHL)	1	6
Project Travel	TBD 2020	Salt Lake City, UT/Eglin AFB (VPS)	1	6
Project Travel	TBD 2020	Portland AFB/JBSA TX (SAT)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH (DAY)/Travis AFB CA (SFO)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH (DAY) /Edwards AFB CA (BUR)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Davis Monthan AFB AZ (TUS)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/ Canon AFB NM (LBB)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Vance AFB OK (OKC)	1	6

Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Dyess AFB TX (LBB)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Keesler AFB MS (GPT)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/MacDill AFB FL (TPA)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Vance AFB OK (OKC)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Good Fellow AFB TX (SJT)	1	6
Site Visit/ Server Install	TBD 2019	Wright Patterson AFB OH/Tyndall AFB CA (ECP)	1	6
Site Visit/ Server Install	TBD 2019	Tampa FL/Lakenheath AB UK (NWI)	1	6
Site Visit/ Server Install	TBD 2019	Tampa FL/ Ramstein AB GM (FRA)	1	6
Site Visit/ Server Install	TBD 2019	Portland OR/Misawa AB JP (MSJ)	1	6
Site Visit/ Server Install	TBD 2019	Portland OR/Osan AB RK (ICN)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Aviano AB IT (TSF)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Anderson AB (GUM)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Incirlik AB (ADA)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Laughlin AFB (PDS)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Barksdale AFB (SHV)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Eglin AFB (VPS)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Patrick AFB (MLB)	1	6
Site Visit/ Server Install	TBD 2019	Salt Lake City UT/ Seymour Johnson AFB (RDU)	1	6

Site Visit/ Server Install	TBD 2020	Tampa, FL/ Scott AFB (STL)	1	6
Site Visit/ Server Install	TBD 2020	Tampa FL/Beale AFB (SMF)	1	6
Site Visit/ Server Install	TBD 2020	Tampa, FL/ McConnel AFB (TUL)	1	6
Site Visit/ Server Install	TBD 2020	Tampa, FL/ Grand Forks AFB (GFK)	1	6

2.11.7. Travel must be coordinated and authorized by the Contracting Officer Representative prior to incurring costs. Contractor costs for travel will be reimbursed in accordance with FAR 31.205-46, in arrears. The travel costs shall be reasonable and allowable as defined in FAR 31.201 and in accordance with the limitations of the DoD Joint Travel Regulations.

2.11.8. The contractor shall invoice monthly on the basis of cost incurred. The contractor must provide documentation in support of all travel expenses. The contactor will not be reimbursed for local travel (within a 50-mile radius of the Government/contractor's facility) or commuter travel (commute from home to work site). Invoice submissions including travel costs shall include completed travel expense sheets (i.e., travel voucher) for each trip and each employee who traveled. The travel expense report, receipts of $75 or more (with exceptions being lodging and transportation), and supporting documentation (e.g., approval email for exceeding per diem rates, cost comparisons, etc.) shall be submitted with the invoice. Expense report(s) must include the traveler's name, dates of travel, destination, purpose of travel, Approval Authority documentation (e.g., copy of the e-mail authorizing travel by Government official), and cost for each trip. All travel costs shall be compiled into a travel expense sheet that has been determined to be acceptable by the Government. The entire submission shall be complete and organized to enable the Government to complete an efficient review. Submissions that are not complete and organized are subject to rejection.

2.11.9. The Contractor shall travel using the lowest cost mode of transportation commensurate with the mission requirements. When necessary to use air travel, the Contractor shall use the tourist class, economy class, or similar lodging accommodations to the extent they are available and commensurate with the mission requirements. Travel shall be reimbursed on a cost basis, no profit or fee shall be paid.

2.12. Mission/Emergency Essential. None of the services listed in this PWS are mission/emergency essential.

2.13. COR Notification of Contractor Employee Absences. Contractor personnel are requested to provide a courtesy notification for any scheduled or unscheduled absences due to illness, incapacitation, emergency, vacation or other inability to work during core hours to the COR or the designated Government official within one (1) hour of the scheduled start of their workday schedule.

2.14. Conduct of Contractor Personnel. The CO or COR may require the contractor to remove

Contractor personnel working under this contract from the job site. Removal from the job site or dismissal from the premises shall not relieve the contractor of the contract requirements.

2.14.1. Contractor personnel shall be required to observe Government facility parking, safety and traffic regulations that apply to all facility employees.

2.14.2. Alcoholic beverages and illegal drugs are prohibited on the job.

2.14.3. There shall be no loud, profane or abusive language used on the job.

2.14.4. Contractor personnel shall present a neat well-groomed appearance. Neat, clean, casual business attire shall be worn.

2.14.5. Contractor personnel must portray a professional demeanor in the office environment.

2.15. Procedures for Payment. Invoices are due no later than the 20th calendar day of the month following the reporting period. The contractor shall submit the invoices and supporting documents, through ITSS simultaneously with the Monthly Status Report (as an acceptance item) to allow the client and the COR to electronically accept and certify services received by the client representative. The contractor is authorized to invoice only for the services and travel authorized under this GSA Task Order and provided in direct support of the contract. Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government. The invoice shall include but not be limited to:

- Clear identification of all costs.
- Labor hours expended (for labor hours tasks). The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Travel costs.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the JTR (receipts for all costs $75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee. All travel costs shall be compiled into the travel expense sheet. The travel expense sheet shall be submitted with the invoice.
- The contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) billing requests.

2.16. Personal Service. The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this contract is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled “Personal Services Contract”. The Contractor agrees that this is a non-personal services contract. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government. The Contractor agrees that his/her personnel shall neither supervise nor accept supervision from Government employees. The Government will not control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are

perceived to constitute personal services, it shall be the contractor's responsibility to notify the Contracting Officers immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government.
2.16.1. Additionally, the Contractor shall take the following steps to preclude performing, or perception of performing "Personal Services" as stipulated in FAR 37.114(c).
2.16.2. When answering the phone, Contractor employees shall identify themselves as employees of the firm for which they work, as well as giving other information such as their name or the government office they support.
2.16.3. Contractor employees shall wear badges that clearly identify them as Contractor employees, in accordance with established Air Force badge requirements. The badge shall be worn on the outermost garment between the neck and waist so badge is visible at all times.
2.16.4. Name plaques shall be placed at Contractor employees' work area (cubical or office) that clearly identify them as Contractor employees. The plaques shall be placed in a clearly visible location so they can be seen by all visitors and associated government employees.

2.17. Section 508. The Contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities.

2.18. CPARS Self-Evaluation. The contractor may submit a self-evaluation of their performance as requested by the GSA COR at least annually utilizing a Government provided template. The contractor self-evaluation will then be submitted to the customer where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

3. CONTRACT REQUIREMENTS

3.1. DICE Support Services – CLIN 01 - FFP: The Contractor shall provide services to support the Government with the management of DICE. The Contractor shall employ a staff with the experience and expertise to perform each of the tasks described below. The Contractor shall be solely responsible for managing the work performed in the execution of the tasks to include assigning appropriate resources to each aspect of the work at each location. The Contractor shall coordinate all work with Government representatives. The Contractor shall assist with the management of all current and pre-defined future technologies. Current USAF dental technologies are built around multiple commercially available products. Existing platforms include 2D and 3D imaging, computer-aided design and computer-aided manufacturing (CAD/CAM), Visual Light Imaging, Healthcare Artifact and Imaging Management Solution, and various data connections/exchanges with the Army and Navy Dental Services. Pre-defined solutions the AF DITAG will manage include 1) the bi-directional connection with the DHA global PACS repository , 2) migration of AF/ANG clinics to the DHA network, 3) integration with MHS

GENESIS (Dentrix Enterprise), and 4) dental radiology reading service, and lab management software. The tasks described in this section identify known design, integration, deployment, sustainment and professional IT services the Contractor shall be required to perform in support of DIT solutions utilized by all AFDS components. The AFDS components include collocated/non-collocated AFRC bases and the ANG Office of the National Guard Bureau Joint Air Surgeon's Office (NGB/SG) units. Work shall be performed remotely or at government facilities and remote locations as necessary. Locations will be designated and approved by AFMOA/SGD and NGB/SG where appropriate. Required data deliverables (reports, studies, presentation materials, etc.) are listed below and in PWS section 6.

3.1.1. Support of the AF DIT Program Leadership and Strategic Planning: The contractor shall designate one FTE to be the Government primary point of contact for DIT senior consultation services and be responsible for the management, content, and quality of work performed. The Contractor shall provide a competent backup for project management in the event of a temporary absence and a competent replacement in the event of an extended absence of the primary contractor (more than two weeks or other time as agreed between the parties). The contractor must hold or fulfill within two (2) weeks of hiring, the requirement of DoD Directive 8570 to obtain an Administrator account on both MedCOI and AFNET. Contractor SC/PM support responsibilities and performance tasks for AF DITAG IT planning and execution functions follow:

3.1.1.1. Primary Focus – Consultation and Project Management:

Function as the Contractor's single POC for AF/ANG leadership. Possess a manager level of knowledge and experience of Digital Dental Radiology and dental DICOM/PACS including MiPACS software, DIT hardware, and FDA approved dental devices. Possess manager level of knowledge experience in management and coordination in a fixed price contract environment within DoD with knowledge of Air Force management practices and program implementation. Possess a manager level of experience in DIT technical knowledge and leadership as demonstrated by participation in nationally recognized DIT forums.

3.1.1.1.1. Provide DIT consultation to AFDS leadership, specifically the AFDS DIT Program Management Office (DITPMO).

3.1.1.1.2. Support other related DIT tasks as determined by the Consultant to the AF Surgeon General for Dental Technology Integration and AFMOA/SGD. These tasks include, but are not limited to, consultative services, advice, and evaluations of new dental technology to support a decision to use or integrate the new technology.

3.1.1.1.3. Provide guidance to the AF DITAG program regarding inter-service integration, evaluations of new technology, hardware and software upgrades/roll-outs to the AF, equipment refreshes, and other DIT operations.

3.1.1.1.4. Provide strategic planning, guidance, and execution for the sustainment, maintenance, and future direction of all AF DIT solutions worldwide, as required by AF Leadership.

3.1.1.1.5. Provide technical leadership in troubleshooting issues with DIT solutions. Coordinate contractor, Subject Matter Experts (SME) and vendor resources to restore service delivery.

3.1.1.1.6. Travel to AF and ANG sites, as needed, for site evaluations and to resolve technical issues.

3.1.1.1.7. Participate in providing consultative services during AFMOA and ANG leadership meetings concerning the AF DITAG and ANG programs.

3.1.1.1.8. Following the direction of AFDS leadership, interface with other DoD services and vendors to advance the technical priorities of the AFDS. Attend meetings and conferences as the AFDS technical SME. Participate in teleconferences with AF, DHA, Army and Navy

representatives.

3.1.1.2. DHA Dental Integration:
3.1.1.2.1. Provide oversight and guidance for the interfacing of the AF DITAG program with AF, Army, and Navy applications/initiatives such as Corporate Dental Application (CDA), Digital Enterprise Viewing & Acquisition Application (DEVAA), Cone Beam technology, etc., for a global solution.
3.1.1.2.2. Provide oversight and guidance for the planning and execution of dental image sharing across the military branches as well as the U.S. Department of Veterans Affairs (VA).
3.1.1.2.3. Lead the integration of dental technologies used in the AF with MHS GENESIS.
3.1.1.2.4. Lead the migration of dental technologies from the AF network to the DHA network, Medical Community of Interest (MedCOI).
3.1.1.3. Contractor Resource Allocation:
3.1.1.3.1. Ensure contract team resources are properly aligned with the needs defined by AF/ANG leadership. Possess the knowledge and experience to manage project tasks and coordination of contract employees in multiple labor categories and various skills in projects of size and scope as identified in this requirement.
3.1.1.3.2. Manage upgrades and roll-outs of hardware and software across the AF and ANG sites within the AF DITAG program.
3.1.1.3.3. Manage the planning and execution of future AF and ANG technical equipment selections, deliveries, and installations at AF and ANG sites.
3.1.1.3.4. Manage AF DITAG technical support to AF and ANG sites to ensure thorough and responsive assistance is provided from the AFMOA DITAG Help Desk.
3.1.1.3.5. Coordinate the efforts of dental industry SMEs on an as-needed basis to provide guidance and potential solutions for issues that may impact the ability of AFDS to meet critical mission requirements.

3.1.2. Information Security Support for AF DIT Cyber Security: Contractor shall manage the System Information Security for DIT systems and act as the liaison to DHA/AF/Air Forces Central Command (AFCENT)/ANG/AFRC/Army/Navy Cyber Security. Contractor will possess Specialist Level knowledge and expertise in cybersecurity oversight of all security operations for a Program Office. A current Certified Information Systems Security Professional (CISSP) and within two weeks of hiring, hold or fulfill a current DoD Directive 8570 IAM Level III baseline certification to function as the ISSM for multiple AF DITPMOs and obtain an Administrator account on both AFNET and MedCOI. The following tasks are required:
3.1.2.1. Primary Focus – Cyber Security Implementation and Sustainment:
3.1.2.1.1. Manage all information security operations:
3.1.2.1.1.1. Implement and ensure security and compliance policies as defined by USAF and DHA Cyber Security across all DIT managed by AF DITPMO.
3.1.2.1.1.2. Ensure appropriate security controls are in place to protect all AF DIT systems and data. Protect against inappropriate access, issues with data integrity, and loss of data confidentiality.
3.1.2.1.1.3. Maintain compliance with all HIPAA policies and procedures to protect confidential patient information.
3.1.2.1.2. Possess specialist level technical and functional expertise of: DoD Cyber Security compliancy tools to include Host Based Security Systems (HBSS), SCCM, SCAP, and eMASS, ACAS and Nessus Cybersecurity compliance tools, and the DIACAP system transition to a RMF

system.

3.1.2.2. Cyber Security Accreditation:

3.1.2.2.1. Achieve and maintain Risk Management Framework (RMF) accreditation for DITPMO systems and enclaves working with DHA Cyber Security (DHA IV&V).

3.1.2.2.1.1. Complete Security Risk Assessments to add software, hardware and Approved dental devices to the RMF accredited systems and enclaves.

3.1.2.2.1.2. Meet deadlines for re-certification of all DIT systems as required by the DHA Cyber Security team.

3.1.2.2.1.3. Manage System of Record instances in DHA Enterprise Mission Assurance Support Services (eMASS) for each dental technology system required by AFMOA/SGDS to maintain compliance with DHA cyber security requirements.

3.1.2.2.1.4. Maintain the Ports and Protocols list of all supported DIT systems

3.1.2.2.1.5. Write the security architecture documentation for all DIT systems.

3.1.2.2.1.6. Work with the team to develop, maintain and test the Disaster Recovery Plans for all DIT systems.

3.1.2.3. Cyber Security Sustainment:

3.1.2.3.1. Lead the AF DITAG team in monitoring and remediation efforts to ensure that all AF DIT systems are regularly patched and configured according to current Defense Information Systems Agency (DISA) Security Technology Implementation Guide (STIG) standards.

3.1.2.3.2. Perform and oversee the Information Systems Security Officers (ISSOs) performing monthly Nessus® Vulnerability Scanner & Security Content Automation Protocol (SCAP) scans.

3.1.2.3.3. Maintain RMF documentation weekly as changes occur making updates to the Security Plan, Boundary Diagram, Ports and Protocols, and Plan of Action & Milestones inside DHA eMASS.

3.1.2.3.4. Perform annual documentation update/review and submit for signature as needed: Privacy Impact Assessment, Public Key Infrastructure PKI) Application Security Plan, Service Level Agreements, and Memorandum of Understanding.

3.1.2.4. Cyber Security Documentation:

3.1.2.4.1. Provide clear and concise documentation for processes, procedures, and policies required by the DHA RMF process to maintain Cyber Security and Readiness

3.1.2.4.2. Respond to queries from AFCENT/A6, AFRC/A6 and NGB/A6 to ensure they have completed lists of any operating system (OS)/hardware configuration changes for DIT systems.

3.1.2.4.3. Provide relevant Cyber Security documents to local MTF Systems supporting inspection preparation or base Communication Squadron inquiries during inspections.

3.1.2.5. Cyber Security Incident Response:

3.1.2.5.1. Plan, deploy, administer, monitor, and provide cybersecurity incident response, IAW guidance provided in the Chairman of the Joint Chiefs of Staff Manual, CJCSM 6510.01B, across the portfolio of Information Systems managed by AF DITPMO.

3.1.2.5.2. Develop operational processes around incident responses to include alerts, escalation, triage, remediation and restoration.

3.1.2.6. Cyber Security Technical Advice:

3.1.2.6.1. Provide technical advice to the DITPMO and AFDS leadership on Cyber Security topics.

3.1.2.6.1.1. Participate in the analysis, evaluation and development of enterprise long-term strategic and short-term tactical plans to ensure that AF DIT objectives are consistent with AFDS leadership's long-term health care objectives while maintaining a strong Cyber Security posture.

3.1.2.6.2. Provide strategic Cyber Security advice to AFDS leadership on the cyber security challenges related to new technologies and FDA certified dental (medical) devices being

investigated for use by the AF.
3.1.2.6.3. Assist AFDS leadership in evaluating the security posture of competing products.
3.1.2.6.4. Participate in security discussions with DHA, Army, and Navy related to the design, development and maintenance of AF DIT. Attend meetings and conferences as the AFDS cyber security SME. Participate in teleconferences as the AFDS cyber security SME.
3.1.2.7. Team Training:
3.1.2.7.1. Provide technical support and train the AF DITAG staff on security vulnerabilities, remediation, and mitigating technologies.
3.1.2.8. Reporting:
3.1.2.8.1. Present to AFDS leadership the following:
3.1.2.8.1.1. Security proposals that align with business objectives as well as time, resource, and cost implications.
3.1.2.8.1.2. Ongoing security compliance, project plans, costs, and delivery dates.
3.1.2.8.1.3. Incident and compliance reports.

3.1.3. Enterprise Architecture / Data Center Management for Central Systems Administration: Contractor shall provide sustainment for the DIT systems chosen by the AFDS leadership. Sustainment includes the hardware and COTS software installation, configuration, and optimization for the AF/AFRC/ANG environment. It also includes planning, installation, configuration and sustainment of the data center technology housed at the Global/Regional Repositories. Contractor will: 1. Hold or fulfill, within two weeks of hiring, the requirements of DoD Directive 8570 to obtain an Administrator account on both AFNET and MedCOI; 2. Possess Specialist Level knowledge and expertise to manage the design, deployment and sustainment of Information Technology to include Windows and Linux Server Platforms, Server Virtualization, Fiber Channel SAN deployments, and Load Balancers; and 3. Possess technical and functional knowledge VMWare ESX & VCenter, EMC VNX, and F5 Load Balancer deployment, configuration, security hardening, and management. The following tasks are required:
3.1.3.1. Enterprise Architecture and Design:
3.1.3.1.1. Recommend and participate in the evaluation and development of enterprise long-term strategic and tactical plans to ensure that AF DIT objectives are consistent with Air Force Dental Leadership long-term health care objectives.
3.1.3.1.2. Recommend and participates in activities related to the design, development and maintenance of AF DIT.
3.1.3.1.3. Lead the technical investigations of potential solutions needed by the AF DITPMO to meet the operational goals of the AFDS.
3.1.3.1.4. Share best practices, lessons learned and update the technical system architecture requirements based on changing technologies, and knowledge related to recent, current and up-coming vendor products and solutions to ensure the technical system remains as up to date as possible.
3.1.3.1.5. Collaborate with all relevant parties in order to review the objectives and constraints of each solution and determine conformance with AF DIT.
3.1.3.1.6. Recommend and participate in the development of architecture blueprints for design and integration of AFMS systems.
3.1.3.1.7. Participate in Proof of Concept projects; thoroughly investigating the architectural solutions to deliver new technology.
3.1.3.1.8. Manage contractor resources that support the Global/Regional data centers hosting the suite of DIT systems required by the AFDS.

3.1.3.1.9. Provide technical consulting on tri-service applications/initiatives that interface with the AF DIT solutions such as CDA, DEVAA, Cone Beam technology, etc.
3.1.3.1.10. Provide technical expertise for dental image sharing across DHA as well as the VA.
3.1.3.1.11. Attend and participate in industry conferences to gather information on AF initiatives and their impact on AF DIT, as well as the latest vendor technology for potential incorporation into the AF DIT program.
3.1.3.2. Data Center Management and Sustainment:
3.1.3.2.1. Maintain the DIT survivability by implementing and maintaining a backup solution which is backed up on a daily basis.
3.1.3.2.2. Maintain the Access, Integrity, and Confidentiality of the PII/PHI stored and transported through the DIT systems in the Global/Regional data centers.
3.1.3.2.3. Configure and maintain replication of all DIT systems between the two Global/Regional Repositories.
3.1.3.2.4. Develop, maintain, and monitor image replication from the dental clinics.
3.1.3.2.5. Configure, maintain, and monitor the server fleet at the Global/Regional Repositories to include security patch installation, security scanning and remediation, and OS upgrades.
3.1.3.2.6. Create and test disaster recovery strategies for all DIT systems.
3.1.3.2.7. Administer the Microsoft Structured Query Language (SQL) Server at the Global/Regional Repositories.
3.1.3.2.8. Maintain compliance with HIPAA policies and procedures, as stored data may contain sensitive or confidential patient information.
3.1.3.2.9. Provide support for attaining and maintaining Cyber Security certification and accreditation.
3.1.3.2.10. Maintain configuration documentation for all DIT systems and supporting infrastructure systems.
3.1.3.2.11. Provide status reporting for all DIT systems and compile Global/Regional Repository statistics.
3.1.3.3. Clinic Server Engineering:
3.1.3.3.1. Configure and test all hardware and software for use at AF/AFRC/ANG clinics.
3.1.3.3.2. Work with the ISD to complete Risk Assessment testing of all software/firmware upgrades.
3.1.3.3.3. Perform functional testing of new software features using SMEs from the Active Duty AF component or relying on the expertise of the Health Information Technology Functional Tester.
3.1.3.3.4. Oversee evaluations and testing for AF and ANG DIT system upgrades, new versions, etc.
3.1.3.3.5. Write detailed descriptions of user needs, system functions, and steps required to develop or modify systems that are a part of the AF and ANG DIT.

3.1.4. Systems Engineer Support for Worldwide AF / ANG Systems Management and Technical Support: Provide systems engineering, analysis and technical support to the DIT solutions deployed worldwide. Contractor(s) must hold or fulfill, within 2 weeks of hiring, the requirements for completion of DoD Directive 8570 to be able to obtain an Administrator account on both AFNET and MedCOI. Contractor(s) must hold Microsoft Certified Solutions Expert (MCSE) certification or equivalent. Contractor(s) must possess Senior and Intermediate technical and functional experience with: 1. A distributed PACS environment such as Medicor Imaging's MiPACS Storage Server Manager, and Client Viewer; 2. The administration of MS Windows Server and MS SQL Server systems, Linux Servers, Server Virtualization, Storage Area Networks,

backup and disaster recovery strategies, and other common data center technologies; 3. DoD Cyber Security compliancy tools including HBSS, SCCM, SCAP, eMASS, ACAS and the Nessus scanning component; 4. VMWare ESX & VCenter, EMC VNX and F5 Load Balancer deployment, configuration, security hardening, and management; and 5. MS Windows Server 2008R2, Windows Server 2012R2 and Windows Server 2016. The following tasks are required for ALL personnel providing Systems Engineers support:

3.1.4.1. DIT Tier 3 Technical Support:

3.1.4.1.1. Provide day-to-day AF DIT Technical Support to AF and ANG sites worldwide for all hardware and software aspects of the AF and ANG DIT systems. Provide Tier 2 Help Desk support to ANG sites during primary and secondary drill weekends. Identify, research, and resolve DIT technical problems.

3.1.4.1.2. Ensure that all email queries and phone calls are handled within one (1) business day.

3.1.4.1.3. Escalate issues to vendor support as needed.

3.1.4.1.4. Work with AF Network Operation Security Centers (NOSCs) to resolve Global Repository connectivity issues.

3.1.4.1.5. Maintain both direct (phone) and indirect (email) contact with AFRC systems personnel to provide assistance in troubleshooting and maintaining access to the Central Repository.

3.1.4.2. DIT System deployment:

3.1.4.2.1. Support Enterprise Architect with building, securing, and shipping new DICE servers. System Engineers are expected to perform the functions under the guidance and oversight of the Enterprise Architect.

3.1.4.2.2. Support AF and ANG DIT installations. In some cases assisting remotely and in some cases traveling to the clinic for the server migration.

3.1.4.2.3. In the case of DICE servers being deployed on Virtual Server Resource Pools at clinic MTFs, support installation of all software, configuration of settings, and functional testing. Provide support remotely for small clinics and in combination with a site visit for larger clinics.

3.1.4.3. DIT System Monitoring and Sustainment:

3.1.4.3.1. Proactively monitor and tune 176 DIT systems for reliable performance. Systems are located at AF and ANG clinics worldwide:

3.1.4.3.1.1. Monitor 176 DIT applications five (5) times a day for successful DICOM traffic and DICOM errors.

3.1.4.3.1.2. Using the checklists provided by the Information Security Director (ISD), maintain the security posture of all AF and ANG servers.

3.1.4.3.1.3. Perform monthly health checks on 176 DICE clinic PACS servers. Confirm DIT System configuration and check log files for errors. Apply Microsoft security patch updates monthly. Reboot server as needed. Flex patch installation and reboot to off-duty hours of the clinic. Perform SCAP scans creating a checklist for upload to DHA eMASS.

3.1.4.3.1.4. Perform quarterly health checks on 176 DICE clinic PACS servers. Update the SCAP engine and install new STIG files. Review the Assured Compliance Assessment Solution (ACAS) report to confirm compliance. Remediate security vulnerabilities if present. Perform firmware upgrades as required, driver upgrades, and application software upgrades.

3.1.4.3.1.5. Verify that the DIT servers at clinics scheduled for an inspection are patched and remediated.

3.1.4.4. DIT Training and Reporting:

3.1.4.4.1. Provide DIT training during site visits at AF and ANG clinics, per the request of either AFMOA/SGDS or NGB/SG.

3.1.4.4.2. Conduct DIT on line training for MTF systems or dental personnel when requested.

3.1.4.4.3. Create reports for DICOM image storage statistics to be viewed by management to determine usage of the AF, ANG, and AFRC clinics.

3.1.4.5. Additional Tasks for Support of ANG Systems Management:

3.1.4.5.1. Tier 3 Systems Administration and Application Support. Provide Tier 3 support to the ANG dental and systems units. Investigate and troubleshoot issues that require escalation to Tier 4 Senior Systems Administration and Application Support. Lead ANG DIT support coordinating activities of System Engineer for ANG. Work with ANG A6 Systems team to maintain connectivity with all DICE servers in ANG. Solve ANG workflow issues.

3.1.5. Systems Engineer Support to Support Worldwide Systems Management:

3.1.5.1. Tier 4 Senior Systems Administration and Application Support. Contractor(s) must hold or fulfill, within 2 weeks of hiring, the requirements for completion of DoD Directive 8570 to obtain an Administrator account on both AFNET and MedCOI. Contractor holds Microsoft Certified Solutions Expert (MCSE) certification or equivalent. Contractor must possess Specialist Level functional knowledge and experience with: 1. A distributed PACS environment such as Medicor Imaging's MiPACS Storage Server Manager, and Client Viewer; 2. Administering MS Windows Server and MS SQL Server systems, Linux Servers, Server Virtualization, Storage Area Networks, backup and disaster recovery strategies, and other common data center technologies; 3. DoD Cyber Security compliancy tools including HBSS, SCCM, SCAP, eMASS, ACAS and the Nessus scanning component; and 4. VMWare ESX & VCenter, EMC VNX and F5 Load Balancer deployment, configuration, security hardening, and management. The following tasks are required:

3.1.5.1.1. Provide Tier 4 support to the AF DIT Tier 2 Helpdesk.

3.1.5.1.2. Research and solve technical and application issues that are referred from Tier 3 engineers.

3.1.5.1.3. Work with hardware and application support personnel to resolve issues.

3.1.5.1.4. Investigate and troubleshoot issues that require escalation to the COTS vendor's Help Desk.

3.1.5.1.5. Coordinate monthly calls with application manufacturers to track bug reports/fixes and feature requests.

3.1.5.1.6. Lead the Systems Engineers in deployment of technical solutions.

3.1.5.1.7. Provide on-going mentoring to the Systems Engineers and the AF DITAG Help Desk staff.

3.1.5.2. Systems Analyst Application Support:

3.1.5.2.1. Perform system analyst activities for all AF DITAG systems.

3.1.5.2.2. Quarterly, work with the Systems Integration Consultant to evaluate all deployed systems identifying any workflow challenges and design solutions.

3.1.5.2.3. Quarterly, modify configurations to optimize application functionality and develop recommendations for feature requests or new software purchases.

3.1.5.3. Application Configuration and Packaging Support:

3.1.5.3.1. Participate in solution design and vendor evaluation of COTS software products.

3.1.5.3.2. Test DIT upgrades and bug fixes to validate functional and technical requirements.

3.1.5.3.3. Interact with software and hardware vendors to understand limitations and configuration requirements for COTS software.

3.1.5.3.4. Along with other senior members of the DITAG participate in technical research and development to enable continuing innovation within AF DIT.

3.1.5.3.5. Support security certifications/re-certifications of all AF DITAG systems.

3.1.5.3.6. Ensure that the configuration design of new system hardware, operating systems, and

software applications adhere to Air Force Cyber Security Standards.
3.1.5.3.7. Quarterly, produce and maintain installation/configuration checklists for all systems.
3.1.5.3.8. Quarterly, using InstallShield, build and maintain silent software installation packages for all DIT applications. Test packages on both AF and DHA networks. Work with AF and DHA System Center Configuration Manager (SCCM) teams, to test and publish the InstallShield packages via SCCM.
3.1.5.3.9. Enhance DIT functionality, improve DIT performance, and ensure that all DIT properly interfaces with other systems.
3.1.5.3.10. Meet new requirements dictated by technology or security changes on AF Network (AFNET) and MedCOI.
3.1.5.3.11. Quarterly track COTS software improvements and recommend upgrades when the new features significantly enhance the capabilities of the AFDS.
3.1.5.3.12. Evaluate and design integration solutions that connect AF DIT with other AFMS or DHA systems.
3.1.5.3.13. Perform DIT hardware and software upgrades and/or oversee upgrades managed by DHA Systems Deployment.
3.1.5.3.14. Provide adjusted resource allocation or additional resource requirements when new expectations from either DHA Cyber Security or AFDS significantly change the scope of work.
3.1.5.4. Application Support:
3.1.5.4.1. Ensure DIT Uptime. Perform necessary functions to ensure maximum DIT accessibility, with the goal of an uptime of 24 hours a day, seven (7) days a week.
3.1.5.4.1.1. Devise and test contingency plans to meet unexpected DIT interruptions.
3.1.5.4.1.2. Routine maintenance downtime shall be scheduled during times of minimal system use taking into consideration the AFRC and ANG weekend drill schedule.
3.1.5.4.1.3. Train the AF DITAG team in new hardware and software solutions.
3.1.5.4.1.4.Oversee implementation of software updates and produce user training and documentation
3.1.5.5. Data Base Administration:
3.1.5.5.1. Install, configure, optimize, and sustain the MS SQL database servers at the global repository and on each of the 176 MTF PACS servers.
3.1.5.5.1.1. Complete upgrades as needed to keep the SQL installations up to date.
3.1.5.5.1.2. Work with the application vendors to validate every SQL patch released by Microsoft to confirm that it doesn't impact the applications running on the server.
3.1.5.5.1.3. Perform Database Administration duties to optimize and sustain the databases running on all of the DICE servers (~178 installations of MS SQL and ~400 databases).
3.1.5.5.1.4. Standardize the MS SQL Server Agent jobs on ~178 MS SQL servers to produce alerts for Cyber Security required topics and system monitoring tasks (approximately 20 Agent jobs per SQL server).
3.1.5.5.1.5. Monitor alert messages from ~178 SQL servers and respond to investigate/resolve issues.
3.1.5.5.1.6. Quarterly, log into each SQL server and perform a Health Check following best practices from Microsoft.

3.1.6. DIT Administrative Assistant Support: Contractor must possess administrative knowledge and skills to support a Program Office within a military/contractor environment. Contractor must possess functional knowledge and experience with Microsoft Office Professional, Visio and Project. Contractor will perform the following administrative functions in support of

AFMOA/SGDS DITPMO and AF DITAG team and functions:
3.1.6.1. Collate, organize, and maintain all project administrative tasks, contract documentation and deliverables.
3.1.6.2. Maintain hard copy and electronic filing systems for all project related work.
3.1.6.3. Set up and maintain schedules, meetings and conferences. Create meeting agendas and take notes at designated meetings for distribution of minutes.
3.1.6.4. Meet and greet AF customers, partners, AF leadership and other guests in person or on teleconferences.
3.1.6.5. Create and modify documents using Microsoft Office Professional and Visio.
3.1.6.6. Develop and maintain Project Plans using Microsoft Project.
3.1.6.7. Develop databases, spreadsheets, and reports that document and track equipment inventories, system statistics and completed tasks.
3.1.6.8. Work with AF leadership and Contractor staff to research and create presentations.
3.1.6.9. Perform general clerical duties to include, but not limited to, photocopying, faxing, mailing, electronic research, editing, and posting of information to SharePoint.
3.1.6.10. Research, price, and purchase contract or office related supplies using ODC funds.
3.1.6.11. Track and assist with expense reports, travel vouchers, monthly reports, annual budget and other time sensitive documents.
3.1.6.12. Support staff in assigned project based work with minimal supervision.
3.1.6.13. Other administrative duties as required.

3.2.Unidentified Optional Support ceiling - CLIN 0002
The contractor shall include the required provisions for Optional support, as defined below, throughout the task order life cycle per the Request for Quote instructions, which includes the requirement for a lump sum CLIN 0002 Optional Labor allotment for Optional Labor support. It is anticipated that the workload will fluctuate, and surge support may be required based on fluid schedule requirements; therefore, the support will be obtained via the utilization of the CLIN 0002 Optional Labor CLIN. Such support may encompass the entire scope of work identified in CLIN 0001, Core Labor AND/OR be similar to the efforts described below. To ensure maximum flexibility with respect to the CLIN 0002 Optional Labor, the contractor shall include a complete price list identifying the proposed hourly labor rates for all labor categories proposed to support CLIN 0001, Core Labor, for the life of the task order. Such rates will be used as the pricing basis to negotiate applicable firm fixed prices for the Optional Labor, when/if needed. The actual time frame for the CLIN 0002 Optional Labor support negotiation and implementation will be dependent upon actual scheduling requirements. Exercising the optional labor requirements will be incorporated via a bilateral agreement to the task order. During the course of the contract, the potential future requirements would be negotiated with the Contractor via a bilateral contract modification. In addition to increased support for CLIN 01, the below future requirements are representative of the potential support to be exercised under this CLIN.

- Global repository hardware may move from Wright Patterson Air Force Base (WPAFB) to the Defense Health Agency (DHA) Data Centers in San Antonio TX and/or Aurora CO. This may require Contractor services being available at these sites.
- Local Picture Archive and Communications System (PACS) servers may migrate from local MTFs to regional Military Healthcare System (MHS) Application Access Gateway (MAAG) Sites requiring the contractor to adjust support services regionally.
- This requirement may transition from an Air Force solution to a tri-service solution. At some point during this contract the three services will be required to rationalize under

DHA and move to a single dental imaging solution.

- Provide Systems Integration Support for DIT (Clinical Systems) to include: assimilation of new software applications and upgrades in the AFDS, collaboration with dental providers and ancillary dental clinical staff, to develop, test, and validate business and clinical workflows as they interface with DIT applications, identification of functional needs and specifications to present to commercial software vendor partners for consideration as improvements to their COTS product, validation of functional testing of all features of the dental applications managed by the DITAG team, and the production of training materials and presentation of in-person and online training sessions.
- Provide as-needed SMEs from the dental industry to provide the AFDS specific input on strategic and tactical decisions and/or to assist with specific projects that further the goals of the AFDS. This support may be provided on an as-needed basis and includes but is not limited to the following tasks: evaluate and provide recommendations to the AF DITPMO and AFMOA/SGD on existing and potentially new dental hardware and software, and develop alternatives and direction for the potential interfacing of the AF DIT with the VA using current Health Information Exchange protocols.
- Provide short term technical engineering support for specific projects requiring specific knowledge of a system or procedure. Technical support shall include some or all of the following functions: assist with AF DIT systems hardware and software configuration and testing, perform quarterly health checks on infrastructure components, provide troubleshooting of unresolved problems with AF DIT systems, and provide on-site support to AF sites, as needed, for project tasks in support of the AF DIT mission. Examples of systems or procedures include, but are not limited to: Maxilliofacial Radiologists, System Integration Consultants for Clinical Systems, Microsoft SQL SMEs and Technical Writers.

3.3. DICE Education and Experience Requirements: The Contractor shall provide qualified personnel capable of providing the professional services necessary to design, implement and sustain the existing Dental Information and Technology program and meet the objectives of this PWS. Contractor employees shall have the following credentials. The Contractor must furnish adequate documentation to substantiate compliance with these requirements and shall certify as to the accuracy and completeness of the supporting documentation. The specialized qualification requirements for each area of expertise are as follows:

3.3.1. General Requirements

3.3.1.1. All contractor employees shall meet the minimum general requirements listed below.
3.3.1.1.1. All contractor personnel shall be capable of working independently
3.3.1.1.2. Strong written and oral communication skills in the English language.
3.3.1.1.3. All contractor employees must be able to read, write, speak and understand English.
3.3.1.1.4. Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
3.3.1.1.5. Exceptional customer service skills.
3.3.1.1.6. Strong time-management and prioritization skills.
3.3.1.1.7. Ability to communicate applicable technical subject matter expertise to management and others.

3.3.2. Specific Expertise and Experience

3.3.2.1. The contractor shall provide personnel with the appropriate skill levels. While each individual contractor employee may not possess expertise and experience in each area below, the Government requires that the overall contractor staff possess the aggregate skills, expertise, and experience in each of the areas identified to successfully complete all task orders.

3.3.2.1.1. Manager level knowledge and experience in Project Management and Senior DIT Consultant services.

3.3.2.1.2. Manger level knowledge and experience to manage project tasks and coordination of contract employees in multiple labor categories and various skills in projects of size and scope as identified in this requirement.

3.3.2.1.3. Manager level of knowledge and experience of Digital Dental Radiology and dental DICOM/PACS including MiPACS software, DIT hardware, and FDA approved dental devices.

3.3.2.1.4. Manager level of knowledge experience in management and coordination in a fixed price contract environment within DoD with knowledge of Air Force management practices and program implementation

3.3.2.1.5. Manager level of experience in DIT technical knowledge and leadership as demonstrated by participation in nationally recognized DIT forums.

3.3.2.1.6. Current DoD Directive 8570 IAM Level III baseline certification to function as the ISSM for multiple AF DITPMOs. Certified Information Systems Security Professional.(CISSP)

3.3.2.1.7. Specialist level knowledge and experience in Cybersecurity Implementation and Sustainment.

3.3.2.1.8. Specialist level knowledge and experience in Cyber Security Accreditation.

3.3.2.1.9. Specialist level knowledge and experience in Cyber Security Incident Response and Technical Advice.

3.3.2.1.10. Specialist, Senior and Intermediate level knowledge and functional experience with DoD Cyber Security compliancy tools to include Host Based Security Systems (HBSS), SCCM, SCAP, and eMASS.

3.3.2.1.11. Specialist, Senior and Intermediate level knowledge and experience with ACAS and Nessus Cybersecurity compliance tools.

3.3.2.1.12. Specialist level knowledge and experience with Enterprise Architecture and Data Center Management for Central Systems Administration.

3.3.2.1.13. Microsoft Certified Solutions Expert (MCSE) certification or equivalent.

3.3.2.1.14. Specialist, Senior & Intermediate level of knowledge and experience with a distributed PACS environment such as Medicor Imaging's MiPACS Storage Server Manager, and Client Viewer.

3.3.2.1.15. Specialist, Senior & Intermediate level of knowledge and experience with administering MS Windows Server and MS SQL Server systems, Linux Servers, Server Virtualization, Storage Area Networks, backup and disaster recovery strategies, and other common data center technologies.

3.3.2.1.16. Specialist, Senior & Intermediate level of knowledge and experience in administering MS Windows Server and MS SQL Server system.

3.3.2.1.17. Specialist, Senior & Intermediate level of knowledge and experience with DoD Cyber Security. Compliancy.

3.3.2.1.18. Specialist ,Senior & Intermediate level of knowledge and experience with MWare ESX & VCenter, EMC VNX and F5 Load Balancer deployment, configuration, security hardening, and management.

3.3.2.1.19. Specialist, Senior & Intermediate level knowledge and experience with MS Windows

Server 2008R2, Windows Server 2012R2 and Windows Server 2016.
3.3.2.1.20. Senior level administrative knowledge and skills to support a Program Office within a military/contractor environment.
3.3.2.1.21. Senior level knowledge and skills Microsoft Office Professional, Visio and Project.

3.4. Dental Information and Technology Security Requirements:

3.4.1. Security Clearance Requirements: All Contractor personnel, except those performing administrative support duties, shall have/obtain an active favorable Tier 3 (T3) – National Agency Check with Local Agency Checks and Credit Check (NACLC) or meet the requirements of DoDM 1000.13-M-VI, January 23, 2014. Contract personnel performing administrative support duties shall have/obtain an active favorable Tier 1 (T1) – National Agency Check with Inquiries/National Agency Check (NACI/NAC) or meet the requirements of DoDM 1000.13-M-VI, January 23, 2014. Cost and documentation required for security certification will be the responsibility of the contractor. The Contractor shall provide documentation received from the appropriate Government agency as to the verification of contract personnel's Tier 1 or Tier 3 certification. In case the certification has been requested, but not received, the Contractor may provide documentation on any Contractor personnel where certification has been requested. In that instance, the Contractor employee will be able to begin work in areas that would not conflict with Government security issues. The COR shall be kept abreast of issues dealing with the Tier 1 and Tier 3 certification. The Contractor's security officer shall ensure timely notification of all hires to the AF SG's Security Office located at the AFMOA/SGA, Joint Base San Antonio (JBSA) Lackland, TX.

3.4.2. List of Contractor Personnel: The Contractor shall maintain a current listing of Contractor personnel. The list shall include Contractor personnel's name, social security number, and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO) and provided to the Information Security Program Manager (ISPM) at each performance site 30 calendar days prior to the service start date. Updated listings shall be provided when Contractor personnel's status or information changes. The Contractor shall notify the ISPM at each operating location 30 calendar days before on-base performance of the service. The notification shall include:
3.4.2.1. Name, address, and telephone number of the company key management representatives.
3.4.2.2. The contract number and contracting agency.
3.4.2.3. The highest level of classified information to which employees require access.
3.4.2.4. The location(s) of service performance and future performance, if known.
3.4.2.5. The date service performance begins.
3.4.2.6. Any change to information previously provided under this paragraph.
3.4.3. Local Area Network (LAN). All Contractor personnel requiring access to the Government unclassified computer network shall have a valid Tier 1 (T1) verified through Joint Personnel Adjudication System (JPAS). No Contractor personnel will be provided access to unclassified computer network or its inherent capabilities (i.e., internet access, electronic mail, file and print services, etc.) without a valid Tier 1 (T1). The Contractor shall be aware of and abide by all Government regulations concerning the authorized use of the Government's computer network including the restriction against using the network to recruit Government personnel or advertise job openings.

3.4.4. Disclosure of Information. In the performance of this contract, the Contractor may have access to data and information proprietary to a Government agency or to another Government

Contractor, or of such nature that its dissemination or use, other than as specified in this contract, would be illegal or otherwise adverse to the interests of the Government or others. The Contractor and its personnel shall not divulge or release data or information developed or obtained under performance of this contract, except to authorize Government personnel or upon written approval of the CO. The Contractor and its' personnel shall not use, disclose, or reproduce proprietary information bearing a restrictive legend, other than as specified in the contract.

3.4.5. USAF/SG Non-Disclosure Agreement (NDA). All Contractor personnel shall sign the NDA provided at Appendix D prior to beginning of contract performance. The Contractor must then provide a copy of the signed/dated NDA to the COR prior to beginning work.

3.4.6. Contractor Manpower Reporting Requirements Application (CMRA). The Contractor shall report ALL contractor labor hours (including subcontracted labor hours) required for performance of services provided under this contract for the Air Force and Army via a secure data collection site. The Contractor is required to completely fill in all required data fields at http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported at any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the CMRA help desk.
3.4.6.1. Uses and Safeguarding of Information. Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the Contractor name and contract number associated with the data.
3.4.6.2. User Manuals. Data for Air Force service requirements must be input at the Air Force CMRA link. However, user manuals for Government personnel and Contractors are available at the Army CMRA link http://www.ecmra.mil.

3.4.7. Government/Contractor Meetings and Reports
3.4.7.1. Post-Award Meeting. The Government will host a post-award meeting with the Contractor within 30 calendar days after contract award via teleconference. The purpose of the meeting is to acquaint all parties including the contracting officer, Government representatives (Program Manager (PM)/COR) and Contractor representatives and review the Contractor's understanding of the requirements, goals and objectives of the contract/task order. The Contractor shall also address the status of any issues that will affect Contractor start-up/ramp-up toward achieving full service/support capability. The Contractor shall provide minutes of this meeting and provide a copy to the COR
3.4.7.2. Initial Contractor Performance Review Meeting. The Contractor shall also attend an Initial Contractor Performance Review 30 calendar days after the Contractor assumes full performance responsibilities (i.e., after completion of transition) to ensure the Contractor has successfully started performance, completed transition, is fully operational, and is within the estimated cost, schedule, and performance parameters of the contract. The Contractor shall provide minutes of this meeting and provide a copy to the COR.
3.4.7.3. Monthly Status Meetings. The Contractor shall participate in monthly status meetings at a mutually agreeable time and place or via teleconference. During these meetings the Contractor shall provide, at a minimum, the following information: accomplishments during the past month; update on work progress and milestones; problems/issues; and planned actions for the coming month. The Contractor shall take minutes of these meetings and include them in the Monthly

Status Report (MSR).
3.4.7.4. Ad hoc Technical/Work Status Meetings. The Contractor shall participate in ad hoc technical meetings to discuss taskings, work progress, technical problems, performance issues, or other technical matters. These meetings will occur at a time and place mutually agreed upon by the parties or via teleconference. Contractor shall take minutes of these meetings and include them in the Monthly Status Report.
3.4.7.5. Contract Administration Meetings. The Contracting Officer (CO) may require the authorized Contractor representative to meet or participate in a teleconference with authorized Government personnel as often as deemed necessary to discuss contract performance or administrative issues. The Contractor may also request a meeting with the CO when deemed necessary. The contractor shall provide minutes of these meetings to the COR.
3.4.7.6. Monthly Status Report (MSR). The Contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the month. Monthly Status Reports shall be rolled up into an Annual Report that is a compilation of MSR reports with specific notable events or report information. The Contractor shall provide at a minimum the following information.
3.4.7.6.1. Summary of effort, progress and status of all activities/requirements by task linked to deliverables as appropriate.
3.4.7.6.2. Accomplishments since the previous Monthly Status Meeting.
3.4.7.6.3. New work added since the previous Monthly Status Meeting.
3.4.7.6.4. Brief summary of activity planned for the next reporting period.
3.4.7.6.5. Deliverables submitted for the period by task and linked to the milestone schedule.
3.4.7.6.6. All standards followed in support of the requirements.
3.4.7.6.7. Staffing.
3.4.7.6.8. Milestone updates and schedule changes, issues and/or variances.
3.4.7.6.9. Problems or issues.
3.4.7.6.10. Government action requested or required.

3.5. Quality Control Plan (QCP). Both the Contractor and the Government have responsibilities for providing and ensuring quality services, respectively. The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this contract are provided as specified in accordance with the applicable Inspection of Services Clause. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The Government has the right to require revisions of the QCP (at no cost to the Government) should the incorporated plan fail to deliver the quality of the services provided at any time during the contract performance. The plan shall include, but is not limited to the following: A description of the inspection system covering all services listed.
3.5.1. The specification of inspection frequency.
3.5.2. The title of the individual(s) who shall perform the inspection and their organizational placement.
3.5.3. A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.
3.5.4. On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:
3.5.5. Date, time, and location of the inspection.
3.5.6. A signature block for the person who performed the inspection.
3.5.7. Rating of acceptable or unacceptable.

3.5.8. Area designated for deficiencies noted and corrective action taken.
3.5.9. Total number of inspections.

3.6. Quality Assurance. The Government will perform periodic reviews of the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements.

4. PERFORMANCE OBJECTIVES.

4.1. Services Summary (SS). The Contractor services requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service for each requirement. These thresholds are critical to mission success.

4.2. Initial Contract Performance Review. The initial evaluation of Contractor performance is a joint determination by the multi-functional team that the Contractor has successfully started performance, completed transition, is fully operational, and is within the estimated cost, schedule, and performance parameters of the contract. The initial evaluation will be conducted by the Government within 30 days after the Contractor assumes full performance responsibilities.

4.3. Services Summary Surveillance.

Performance Objectives	PWS Paragraph	Performance Threshold	Incentive/Disincentive
Maintain RMF documentation weekly as changes occur making updates to the Security Plan, Boundary Diagram, Ports and Protocols, and	3.1.2.3.3.	No more than two (2) substantiated negative feedbacks in a six (6) month period	Positive/Negative Performance Assessment in CPARs
Perform monthly health checks on 176 DICE clinic PACS servers.	3.1.4.3.1.3.	No more than two (2) substantiated negative feedbacks in a six (6) month period	Positive/Negative Performance Assessment in CPARs
Perform quarterly health checks on 176 DICE clinic PACS servers.	3.1.4.3.1.4.	No more than two (2) substantiated negative feedbacks in a six (6) month period	Positive/Negative Performance Assessment in CPARs

The Contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the	3.4.7.6.	No more than two (2) substantiated negative feedbacks in a six (6) month period	Positive/Negative Performance Assessment in CPARs

5. GOVERNMENT FURNISHED PROPERTY (GFP). The Government will provide the Contractor with the facilities, equipment, and information necessary to perform the tasks stipulated in this contract. Contractor personnel assigned to a government facility will be provided office space in unclassified work areas and equipment, including computers unclassified), desks, chairs, access to printers, unclassified networks, copy machines, classified destruction equipment, telephones (secure, DSN, commercial access capabilities), basic office supplies, and Government vehicles, if necessary and available. Contractor personnel authorized to telework will be provided computers and related office equipment such as docking stations, monitors, printers and basic office supplies. Key Contractor personnel will also be issued a government smart phone, e.g. iPhone, to allow access to answer and respond to technical support requests and respond to leadership. These items are incidental to the place of performance and remain accountable to the Government. In addition, the Government shall require each individual Contractor employee to sign hand receipts for all Information Technology Equipment (ITE) that they exclusively use (i.e., all equipment on their desks). This includes laptops for travel or out-of-office use. Contractor employees are not required to sign for multiple users ITE such as network equipment, network printers, and servers. Information includes all reference material or documentation required to perform. All facilities, equipment, and information used by the Contractor will remain the property of the Government and the Contractor shall return all facilities, equipment, and information to the COR or other designated representative upon the request of the Government or at the end of the contract period of performance.

6. DELIVERABLES. The following data items shall be delivered as stipulated in the deliverable table. In the absence of specific delivery information in in the deliverable table, the Contractor shall comply with the following delivery requirements.

6.1. The Contractor shall submit all deliverables as specified in this PWS.

6.2. All deliverables must be submitted electronically to the COR using standard Microsoft Office products (e.g., Word, Excel, PowerPoint, Access etc.) Government personnel will have 10 workdays to review deliverables (to include resubmissions) and provide written acceptance/rejection. Government representatives and/or the applicable Contracting Officer Representatives (CORs) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 days of receipt of comments at no additional cost to the Government. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

6.3. The COR may approve extensions to the delivery timeline based on magnitude and complexity

of the document topic.

6.4. Deliverable Rights. All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination or expiration of the contract. The Government shall retain ownership of all proprietary information and intellectual property generated under this contract.

6.5. Transfer of Ownership. All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor or for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination or expiration of the contract.
6.6. Required reports shall be in the required Government format provided by the COR. The list of reports are:

AIR FORCE DELIVERABLE TABLE			
PWS Section	**Deliverable**	**Delivery Time**	**Deliver To**
2.3.	Contractor Meeting minutes	Five (5) business days after meeting	Electronically to the COR via email
3.4.2.	Staff Matrix A complete and current list of Contractor employees and the task/office/function they are supporting	Furnished at the post award meeting with an update furnished on or before the date of any personnel change.	Electronically to the COR via email
3.4.5.	Contractor Employee Non-disclosure Agreement	After award but prior to commencement of performance by all Contractor personnel	Electronically to the COR via email
3.4.7.1.	Post Award Meeting Minutes	Two (2) business days after the Post Award meeting	Electronically to the COR via email
3.4.7.2.	Initial Contractor Performance Review Meeting minutes	Five (5) business days after meeting	Electronically to the COR via email
3.4.7.3.	Monthly Status Meetings minutes	10 business days after meeting	Electronically to the COR via email
3.35.	Quality Control Plan-Draft	10 business days after award.	Electronically to the COR via email

3.5.	Quality Control Plan-Final	30 business days after Government review. (The Government shall review and provide comments within seven (7) business days after receipt of the draft QCP.)	Electronically to the COR via email
3.4.7.6.	Monthly Status Report	10 business days after the first day of the month.	Electronically to the COR via email
3.4.7.6.	Annual Status Report	30 days after end of the fiscal year.	Electronically to the COR via email
3.4.7.4.	Ad Hoc Meeting minutes	Five (5) business days after meeting	Electronically to the COR via email
2.~~10~~11.~~5~~8.	Trip Report	Five (5) business days after completion of each trip	Electronically to the COR via email

The Contractor shall deliver the data items listed in the table below to the ANG Tech Rep:

AIR NATIONAL GUARD DELIVERABLE TABLE			
PWS Section	**Data Item Title**	**Delivery Time**	**Deliver To**
3.~~3~~4.7.~~7~~6.	Monthly Status Report (ANG focus)	10 business days after the first day of the month.	Electronically by email to: 1. COR 2. ANG Rep
3.~~3~~4.7.~~7~~6.	Annual Summary Report (ANG focus)	30 days after end of the fiscal year.	Electronically by email to: 1.COR 2. ANG Tech Rep
2.~~10~~11.~~5~~8.	Trip reports and After Action Summary (ANG focus)	Five (5) business days after completion of each trip	Electronically by email to: 1.COR 2. ANG Tech Rep

7.0 APPENDICES

APPENDIX A – Acronyms and Definitions
APPENDIX B - DoD Regulations/Manuals/Instructions/Directives
APPENDIX C - Business Associate Agreement
APPENDIX D - HQ USAF/SG Non-Disclosure Agreement

APPENDIX A – Acronyms and Definitions

ACRONYM	DEFINITIONS
ACAS	Assured Compliance Assessment Solution
3D	Three-dimensional
AF	Air Force
AFCENT	Air Forces Central Command
AFDS	Air Force Dental Service
AF DIT	Air Force Dental Information and Technology
AF DITAG	Air Force Dental Information and Technology Action Group
AF DITPMO	AF Dental Information and Technology Program Management Office
AFMOA	Air Force Medical Operations Agency
AFMOA/SGD	Air Force Medical Operations Agency Dental Directorate
AFMS	Air Force Medical Services
AFNET	AF Network
AFRC	Air Force Reserve Command
ANG	Air National Guard
BLS	Basic Life Support
CAD/CAM	Computer-aided Design and Computer-aided Manufacturing
CCRI	Command Cyber Readiness Inspection
CDA	Certified Dental Assistant
CDRL	Contract Data Requirements List
CEUs	Continuing Education Units
CISSP	Certified Information Systems Security Professional
CMRA	Contractor Manpower Reporting Requirements Application
CO	Contracting Officer
CONUS	Continental United States
COR	Contracting Officer Representative
COTS	Commercial-Off-the-Shelf
DDRS/DICE	Digital Dental Radiology Solution/Dental Imaging Collaborative
DECS	Dental Evaluation and Consultation Service
D-EHR	Dental Electronic Health Record (as provided by DHA)
DEVAA	Digital Enterprise Viewing & Acquisition Application
DHA	Defense Health Agency
DICOM	Digital Imaging and Communications in Medicine
DID	Data Item Description
DIT	Dental Information and Technology
DoD	Department of Defense
ECIA	Enterprise Clinical Imaging Archive
eMASS	Enterprise Mission Assurance Support Service

ERM	Electronic Records Management
FDA	Food And Drug Administration
FSO	Facility Security Officer
FY	Fiscal Year
GFP	Government Furnished Property
HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IG	Inspector General
ISPM	Information Security Program Manager
ISD	Information Security Director
ISSM	Information Systems Security Manager
ISSOs	Information Systems Security Officers
IT	Information Technology
ITE	Information Technology Equipment
IV&V	Independent Verification and Validation
JBSA	Joint Base San Antonio
JPAS	Joint Personnel Adjudication System
LAN	Local Area Network
MCSE	Microsoft Certified Solutions Expert
MedCOI	Medical Community of Interest
MHS	Military Healthcare System
MiPACS	Medicor Imaging Picture Archive Communication System
MS	Microsoft
MTF	Military Treatment Facility
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NDA	Non-Disclosure Agreement
NGB/SG	Air National Guard Office of the Air Surgeon
NOSCs	Network Operation Security Centers
OCONUS	Outside Continental United States
PACS	Picture Archive and Communication System
PKI	Public Key Infrastructure
POC	Point of Contact
PoP	Period of Performance
PWS	Performance Work Statement
PM	Program Manager
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol

SCCM	System Control Configuration Monitor
SG	Surgeon General
SQL	Structured Query Language
SME	Subject Matter Expert
SS	Services Summary
STIG	Security Technology Implementation Guide
T1	Tier 1
UEI	Unit Effective Inspection
USAF	United States Air Force
VA	U.S. Department of Veterans Affairs

APPENDIX B - DoD Regulations/Manuals/Instructions/Directives

Department of Defense (DoD) Regulations/Manuals/Instructions/Directives: Publications applicable to this requirement include, but are not limited to, those listed below. The Contractor shall follow all applicable publications and references thereto. Supplements or amendments to listed publications from any organizational level may be issued by the Air Force (AF) Publications Office during the life of the contract.

Publications and forms are maintained and available electronically for Contractor download through the internet.

DoD Directives can be found at http://www.dtic.mil/whs/directives/index.html Regulations are followed by a "---R" (e.g., DoD 6025.18-R) and can be located on the website by clicking on *Publications* instead of *Directives*.

DEPARTMENT OF DEFENSE (DoD) REGULATIONS/MANUALS INSTRUCTIONS/DIRECTIVES
Most current version will apply

PUB NO.	TITLE
DoDD 5015.2	DoD Records Management Program
DoD 5015.02-STD	Electronic Records Management Software

The Air Force's e-Publishing site (http://www.e-publishing.af.mil) shall be used to obtain Air Force Instructions.

AIR FORCE INSTRUCTIONS (AFI)/MANUALS
Most current version will apply

PUB NO.	TITLE
AFI-33-322	Records Management Program
AF Manual 33-326	Preparing Official Communications
AFI 33-364	Records Disposition--Procedures and Responsibilities
AFI 33-360	Publications and Forms Management
AF Handbook (AFH) 33-337	The Tongue and Quill
DoDD 5015.2	DoD Records Management Program
DoD 5015.02-STD	Electronic Records Management Software

APPENDIX C – Business Associate Agreement

This BAA can serve as a separate standalone agreement or may be used for new or existing contracts between the MTF and the business associate.

Business Associate Agreement

[**USE FOR STANDALONE BAA ONLY**] This Business Associate Agreement (this "Agreement") is entered into this ___ day of _____, _____ (the "Effective Date") between [**NAME OF MHS COVERED ENTITY**] ("Covered Entity") and [**NAME OF BUSINESS ASSOCIATE**], a [type of business entity] ("Business Associate").

Introduction

In accordance with 45 CFR 164.502(e)(2) and 164.504(e) and paragraph C.3.4.1.3 of DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003, this document serves as a business associate agreement (BAA) between the signatory parties for purposes of the Health Insurance Portability and Accountability Act (HIPAA) and the "HITECH Act" amendments thereof, as implemented by the HIPAA Rules and DoD HIPAA Issuances (both defined below). The parties are a DoD Military Health System (MHS) component, acting as a HIPAA covered entity, and a DoD contractor, acting as a HIPAA business associate. The HIPAA Rules require BAAs between covered entities and business associates. Implementing this BAA requirement, the applicable DoD HIPAA Issuance (DoD 6025.18-R, paragraph C3.4.1.3) provides that requirements applicable to business associates must be incorporated (or incorporated by reference) into the contract or agreement between the parties.

(a) Catchall Definition. Except as provided otherwise in this BAA, the following terms used in this BAA shall have the same meaning as those terms in the DoD HIPAA Rules: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Breach means actual or possible loss of control, unauthorized disclosure of or unauthorized access to PHI or other Personally Identifiable Information (PII) (which may include, but is not limited to PHI), where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of breach in DoD Privacy Act Issuances as defined herein.

Business Associate shall generally have the same meaning as the term "business associate" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean [**INSERT NAME OF BUSINESS ASSOCIATE**].

Agreement means this BAA together with the documents and/or other arrangements under which the Business Associate signatory performs services involving access to PHI on behalf of the MHS component signatory to this BAA.

Covered Entity shall generally have the same meaning as the term "covered entity" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean [**INSERT NAME OF MTF COMPONENT**].

DHA Privacy Office means the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Director is the HIPAA Privacy and Security Officer for DHA, including the National Capital Region Medical Directorate (NCRMD).

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are DoD 6025.18-R (2003), DoDI 6025.18 (2009), and DoD 8580.02-R (2007).

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (2007) and DoD 5400.11-R (2007).

HHS Breach means a breach that satisfies the HIPAA Breach Rule definition of breach in 45 CFR 164.402.

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 CFR Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-D (Enforcement), as amended by the 2013 modifications to those Rules, implementing the "HITECH Act" provisions of Pub. L. 111-5. See 78 FR 5566-5702 (Jan. 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013)). Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this BAA and are not included in the term HIPAA Rules.

Service-Level Privacy Office means one or more offices within the military services (Army, Navy, or Air Force) with oversight authority over Privacy Act and/or HIPAA privacy compliance.

I. Obligations and Activities of Business Associate

(a) The Business Associate shall not use or disclose Personal Health Information (PHI) other than as permitted or required by this Agreement or as required by law.

(b) The Business Associate shall use appropriate safeguards, and comply with the DoD HIPAA Rules with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.

(c) The Business Associate shall report to Covered Entity any Breach of which it becomes aware, and shall proceed with breach response steps as required by Part V of this BAA. With respect to electronic PHI, the Business Associate shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of this Agreement. If at any point the Business Associate becomes aware that a security incident involves a Breach, the Business Associate shall immediately initiate breach response as required by part V of this BAA.

(d) In accordance with 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), respectively, and corresponding DoD HIPAA Issuances, as applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI.

(e) The Business Associate shall make available PHI in a Designated Record Set, to the Covered Entity or, as directed by the Covered Entity, to an Individual, as necessary to satisfy the Covered Entity obligations under 45 CFR 164.524 and corresponding DoD HIPAA Issuances.

(f) The Business Associate shall make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526, and corresponding DoD HIPAA Issuances.

(g) The Business Associate shall maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or an individual as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.528 and corresponding DoD HIPAA Issuances.

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Privacy Rule, the Business Associate shall comply with the requirements of the HIPAA Privacy Rule that apply to the Covered Entity in the performance of such obligation(s); and

(i) The Business Associate shall make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

II. Permitted Uses and Disclosures by Business Associate

(a) The Business Associate may only use or disclose PHI as necessary to perform the services set forth in this Agreement or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by this Agreement or directed by the Covered Entity **[MODIFY THIS SECTION IF THE PURPOSE OF THE AGREEMENT/CONTRACT IS FOR THE BA TO DEIDENTIFY PHI FOR THE CE]**.

(b) The Business Associate agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances.

(c) The Business Associate shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the Covered Entity, except uses and disclosures for the Business Associate's own management and administration and legal responsibilities or for data aggregation services as set forth in the following three paragraphs.

(d) Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal

responsibilities of the Business Associate. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

(e) Except as otherwise limited in this Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f) Except as otherwise limited in this Agreement, the Business Associate may use PHI to provide Data Aggregation services relating to the Covered Entity's health care operations.

III. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) The Covered Entity shall notify the Business Associate of any limitation(s) in the notice of privacy practices of the Covered Entity under 45 CFR 164.520 and the corresponding provision of the DoD HIPAA Issuances, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522 and the corresponding DoD HIPAA Issuances, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

IV. Permissible Requests by Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Covered Entity, except for providing Data Aggregation services to the Covered Entity and for management and administrative activities of the Business Associate as otherwise permitted by this BAA.

V. Breach Response

(a) In general.

(1) In the event of a breach of PII/PHI held by the Business Associate, the Business Associate shall report the breach to the Covered Entity in accordance with Section VII, assess the breach incident,

take mitigation actions as applicable, and notify affected individuals, as directed by the Covered Entity.

(2) The Business Associate shall coordinate all investigation actions with the Covered Entity, and at a minimum, follow the breach response requirements set forth in this Part V, which is designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves PII without PHI, then the Business Associate shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Business Associate shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Business Associate has no HIPAA breach response obligations. In such cases, the Business Associate must still comply with breach response requirements under the DoD Privacy Act Issuances.

(3) The Business Associate shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Business Associate has caused or is otherwise responsible for addressing.

(b) Government Reporting Provisions

(1) If the Covered Entity determines that a breach is an HHS Breach, then the Business Associate shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Covered Entity, regardless of where the breach occurs. If the Covered Entity determines that the breach does not constitute an HHS Breach, then the Business Associate shall comply with DoD Privacy Act Issuances, as directed by the applicable Service-Level Privacy Office.

(2) This Part V is designed to satisfy the DoD Privacy Act Issuances and the HIPAA Breach Rule as implemented by the DoD HIPAA Issuances. In general, for breach response, the Business Associate shall report the breach to the Covered Entity, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines "breach" to include possible (suspected) as well as actual (confirmed) breaches, the Business Associate shall implement these breach response requirements immediately upon the Business Associate's discovery of a possible breach.

(3) The following provisions of Part V set forth the Business Associate's Privacy Act and HIPAA breach response requirements for all breaches, including but not limited to HHS breaches.

(i) The Business Associate shall report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the Covered Entity, and to other parties as deemed appropriate by the Covered Entity. The Business Associate is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Business Associate.

(ii) The Business Associate shall submit the US-CERT report using the online form at https://forms.us-cert.gov/report/. Before submission to US-CERT, the Business Associate shall save a copy of the on-line report. After submission, the Business Associate shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one hour deadline for submission, the Business Associate shall submit the US-CERT report

by the deadline. The Business Associate shall e-mail updated information as it is obtained, following the instructions at http://www.us-cert.gov/pgp/email.html. The Business Associate shall provide a copy of the initial or updated US-CERT report to the Installation Privacy Act Officer, MTF HIPAA Privacy Officer, and the Contracting Officer (if applicable), if requested. Business Associate questions about US-CERT reporting shall be directed to the Installation Privacy Act Officer or MTF HIPAA Privacy Officer, not the US-CERT office.

(iii) The Business Associate shall comply with the Breach Timeline and Notification Flow Chart processes attached to this Agreement, to include the timelines established for completing the DD Form 2959 and the HIPAA Privacy Incident Report.

(4) If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Business Associate shall inform the Covered Entity as soon as possible if it believes that "single event" breach response is appropriate; the Covered Entity will determine how the Business Associate shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Business Associate report updates, beneficiary notification, and mitigation.

(i) When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Business Associate shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text. Examples of updated information the Business Associate shall report include, but are not limited to: confirmation on the exact data elements involved, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, and follow-up. The Business Associate shall submit these report updates within three (3) business days after the new information becomes available. Prompt reporting of updates is required to allow the Covered Entity to make timely final determinations on any subsequent notifications or reports. The Business Associate shall provide updates to the same parties as required for the initial Breach Reporting Form. The Business Associate is responsible for reporting all information needed by the Covered Entity to make timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy and Civil Liberties Office as required by DoD Privacy Act Issuances.

(ii) In the event the Business Associate is uncertain on how to apply the above requirements, the Business Associate shall consult with the **Covered Entity and Contracting Officer** (if applicable) when determinations on applying the above requirements are needed.

(c) Individual Notification Provisions

(i) If the Covered Entity determines that individual notification is required, the Business Associate shall provide written notification to individuals affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities of the individuals are ascertained. The 10 day period begins when the Business Associate is able to determine the identities (including addresses) of the individuals whose records were impacted.

(ii) The Business Associate's proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph VII for their review, and

for approval by the [**REMOVE CO REFERENCES FOR STAND-ALONE AGMT**] **Contracting Officer, in consultation with the** Covered Entity. Upon request, the Business Associate shall provide the **Contracting officer and** Covered Entity with the final text of the notification letter sent to the affected individuals. If different groups of affected individuals receive different notification letters, then the Business Associate shall provide the text of the letter for each group (PII shall not be included with the text of the letter(s) provided). Copies of further correspondence with affected individuals need not be provided unless requested by the **Contracting Office or** Covered Entity. The Business Associate's notification to the individuals, at a minimum, shall include the following:

(A) The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached.

(B) The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so the individual clearly understands how the breach occurred.

(C) The individual(s) must be informed of what protective actions the Business Associate is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

(F) The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) the Business Associate may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information. The [**REMOVE CO REFERENCES FOR STAND-ALONE AGMT**] **Contracting Officer, in consultation with the** Covered Entity will determine the appropriate level of support services.

(iii) Business Associates shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Important information – do not destroy," and the envelope is marked with the identity of the Business Associate and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated POC to include, phone number, e-mail address, and postal address.

(iv) If the Business Associate determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 day period after discovering the breach, the Business Associate shall so indicate in the initial or updated Breach Report Form. Within the 10 day period, the Business Associate shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within 10 days after their identities and addresses are ascertained. The Business Associate shall consult with the Covered Entity, which will determine which media notice is most likely to reach the population not otherwise identified or reached. The Business Associate shall issue a generalized media notice(s) to that population in accordance with the Covered Entity approval.

(d) Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. In the event of a security incident not involving a PII/PHI breach, the Business Associate shall follow applicable DoD Information Assurance requirements under its Agreement. If at any point the Business Associate finds that a cybersecurity incident involves a PII/PHI breach (suspected or confirmed), the Business Associate shall immediately initiate the breach response procedures set forth here. The Business Associate shall also continue to follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA.

VI. Termination

(a) Termination. Noncompliance by the Business Associate (or any of its staff, agents, or subcontractors) with any requirement in this BAA may subject the Business Associate to termination under any applicable default or other termination provision of **the underlying Contract** [**FOR STANDALONE INSERT, REPLACE WITH** "**this Agreement**"].

(b) Effect of Termination.

(1) If this Agreement has records management requirements, the Business Associate shall handle such records in accordance with the records management requirements. If this Agreement does not have records management requirements, the records should be handled in accordance with paragraphs VI.(2) and (3) below. If this Agreement has provisions for transfer of records and PII/PHI to a successor Business Associate, or if the Covered Entity gives directions for such transfer, the Business Associate shall handle such records and information in accordance with such Agreement provisions or the Covered Entity's direction.

(2) If this Agreement does not have records management requirements, except as provided in the following paragraph (3), upon termination of this Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the PHI.

(3) If this Agreement does not have records management provisions and the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon

mutual agreement of the Covered Entity and the Business Associate that return or destruction of PHI is infeasible, the Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

VII. Notices. Any notices to be given hereunder will be made in the most expedient manner, via e-mail, facsimile, U.S. Mail, or express courier to such party's address given below.

If to the Business Associate:		If to the Covered Entity:	
Attn:		Attn:	
Title:		Title:	MTF HIPAA Privacy Officer
Company:		Unit:	
Address:		Address:	
Phone:		Phone:	
Fax:		Fax:	
E-mail:		E-mail:	

With a copy to:

Name:		Name:	
Company:		Title:	Contracting Officer
Address:		Address:	
Phone:		Phone:	
Fax:		Fax:	
Email:		Email:	

Each party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner provided in this subsection.

VIII. Miscellaneous

(a) Survival. The obligations of Business Associate under the "Effect of Termination" provision of this BAA shall survive the termination of this Agreement.

(b) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity and the Business Associate to comply with the HIPAA Rules and the DoD HIPAA

[**USE FOR STANDALONE BAA ONLY**] (c) Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. The parties acknowledge and agree that faxed and/or electronically affixed signatures shall act as original

signatures that bind each faxing, or electronically affixing, signatory to the terms and provisions of this Agreement. Delivery of an executed counterpart of this Agreement by facsimile or electronic mail shall be equally effective as delivery of a manually executed counterpart.

[**USE FOR STANDALONE BAA ONLY**] (d) Entire Agreement; Amendment. This Agreement embodies the entire understanding between the parties pertaining to the subject matter contained in it; supersedes any and all prior negotiations, correspondence, understandings, or agreements of the parties with respect to its subject matter; and may be waived, altered, amended, modified, revised or repealed, in whole or in part, only on the written consent of the parties to this Agreement.

[**USE FOR STANDALONE BAA ONLY**] IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

BUSINESS ASSOCIATE:		**COVERED ENTITY:**	
Signature:	_____	Signature:	_____
Print name:	_____	Print name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

APPENDIX D - HQ USAF/SG Non-Disclosure Agreement

REVISED: 30 AUG 2007

Purpose: The purpose of this Non-Disclosure Agreement (NDA) is to confirm in writing that the undersigned understands his/her responsibilities regarding protection of information and/or material that he/she may come in contact with in the course of work performed under this agreement. This NDA covers all forms of information made available as Government Furnished Information or information/material developed under this agreement, whether in the form of working materials or as deliverable product. This NDA applies to unclassified Government information/material, proprietary information/material supplied by other vendors for use by the Government, and classified Government information/material and is intended to supplement, not replace, the DD Form 254. All information/material released to the contractor remains the property of the US Government and may be withdrawn at any time.

Responsibility: As a condition of acceptability for work under this agreement on behalf of AF/SG, individuals are required to complete the attached NDA:

APPENDIX D (Continued)

NON-DISCLOSURE AGREEMENT FOR CONTRACTOR/SUBCONTRACTOR EMPLOYEES, SENIOR MANAGERS OR CORPORATE OFFICERS

I,_____(clearly print or type name), an employee, senior manager, or corporate officer of either _____ or a subcontractor to_____under Prime Contract number_____; Task Order_____awarded to _____ by the AF/SG office (Customer) agree not to disclose to any third party or anyone who is not performing work for the Customer and who does not have a need to know such information, any proprietary, source selection sensitive information, programmatic, or budgetary information (Information) contained in or accessible through the AF/SG programs and activities. Proprietary, programmatic, budgetary and source selection sensitive information and data will be handled in accordance with Government direction under the AF/SG program and applicable Government laws and regulations, including Federal Acquisition Regulation (FAR) Sections 3.104 and 9.5.

I understand that Information I may receive or possess, as a result of my assignment to work on AF/SG activities under this Contract may be considered proprietary, source selection sensitive information, and/or For Official Use Only. The responsibilities of my employer for the proper use and protection from unauthorized disclosure of proprietary or source selection sensitive information are described in FAR 3.104. Pursuant to FAR 3.104, I agree that I shall not appropriate such information for my own use or release or discuss such information with third parties unless specifically authorized by the procedures set forth in FAR 3.104.

This Agreement shall continue for a term of five (5) years from the date upon which I last have access to such information. Upon expiration of this Agreement, I have a continuing obligation not to disclose proprietary, programmatic, budgetary or source selection sensitive information to any person or legal entity unless that person or legal entity is authorized by the Government to receive such Information. I understand that any violation of my duty to protect proprietary or source selection sensitive information I was exposed to while working as an employee of _____company working under the Prime Contract, subcontract, or task order as referenced above may subject me, and/or my employer, to administrative, civil and criminal sanctions.

I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action. I understand that another company might file a separate claim against me if I have misused its proprietary information.

In the event that I seek other employment, I will reveal to any prospective employer the continuing obligation in this agreement prior to accepting any employment offer.

If signing as a corporate officer of either the Prime or Subcontractor, I certify that I am a duly authorized representative with legal authority to bind the Company.

Agreed and Accepted:

(Signature of Employee)	(Date)
(Printed Name/Position)	(Telephone Number)
(Signature of Employer Sr. Mgr/Officer)	(Date)
(Printed Name/Position)	(Telephone Number)